M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
Brandon P. Jack (SBN 325584)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
6200 Canoga Ave, Suite 375
Woodland Hills, CA 91367
Telephone: (747) 777-7748
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Justin Walker (*Pro Hac Vice* Forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
jwalker@msdlegal.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

MFOLOZI DLAMINI, individually and on behalf of all others similarly situated,

Plaintiff,

v.

PUMA BIOTECHNOLOGY, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMAND

Plaintiff Mfolozi Dlamini ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Puma Biotechnology, Inc. ("Puma" or "Defendant"), and alleges upon personal knowledge as to his own actions and the investigation of his counsel, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant on behalf of himself and all other persons harmed by the Data Breach that Defendant announced between April 22, 2022 and June 19, 2022 (the "Data Breach").

2. Defendant Puma is a biotechnology company that focuses on "in-licensing innovative drug candidates that are undergoing or have already completed initial clinical testing for the treatment of various forms of cancer and then seek to further develop these drug candidates for commercial use."[1] Puma Biotechnology employs more than 250 people and generates approximately $228 million in annual revenue.[2]

3. Despite marketing itself as a safe repository for sensitive information, Defendant failed to take basic precautions designed to keep that information secure.

[1] https://www.pumabiotechnology.com/about_overview.html/ (last visited May 25, 2023).

[2] https://www.zippia.com/puma-biotechnology-careers-9480/revenue/ (last visited May 25, 2023).

According to Defendant, between April 22, 2022 and June 19, 2022, hackers gained access to the Defendant's systems that it uses to store a wide range of sensitive personal information on its customers including names, Social Security numbers, financial account information, and health insurance information.[3]

4. In May 2023, Defendant began sending letters to affected individuals notifying them that their information was compromised. In those Data Breach notification letters, Defendant admits that information in its systems was accessed by unauthorized individuals. The particular sensitive nature of the exposed data includes medical information, which means Plaintiff and Class Members have suffered irreparable harm and are subject to an increased risk of identity theft for the foreseeable future.

5. Defendant understands that it is required by law to protect such information. For example, on Defendant's website it states in its "Online Services Privacy Policy" that:

> We will take all steps reasonably necessary to ensure that your personal data is treated securely and in accordance with this policy and have put in place appropriate safeguards in accordance with applicable legal requirements to ensure that data is adequately safeguarded and

[3] Exhibit A – "Notice of Security Incident" letter to Plaintiff dated May 17, 2023.

protected irrespective of the country in which the data is processed.[4]

6. The Data Breach was the result of Defendant's failure to implement reasonable policies and procedures to protect the security of the personally identifiable information ("PII") and protected health information ("PHI") it collected as part of its business.

7. Plaintiff and Class Members face an ongoing and lifetime risk of identity theft, which is heightened by the exposure of their medical information.

8. Plaintiff and Class Members have suffered concrete injury as a result of Defendant's conduct. These injuries include: (i) fraudulent misuse of the stolen PII and PHI that is traceable to this Data Breach; (ii) lost or diminished value of PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (v) the present and immediate risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and subject to further unauthorized disclosures if Defendant fails to undertake adequate measures to protect the PII and PHI.

[4] https://pumabiotechnology.com/privacy_policy_20180525.html (last visited May 25, 2023).

II. PARTIES

9. Plaintiff Mfolozi Dlamini is a citizen of Nevada and resides in Reno, Nevada. In May 2023, he received a Data Breach notification from Defendant informing him that his PII and PHI were compromised in the Data Breach. As a consequence of the Data Breach, Plaintiff Mfolozi Dlamini has been forced to and will continue to invest significant time monitoring his accounts to detect and reduce the consequences of likely identity fraud. Plaintiff Mfolozi Dlamini is concerned that he will have to freeze his credit reports to ensure that no one can take out credit in his name. Given the highly sensitive nature of the information stolen, Plaintiff Mfolozi Dlamini suffers present, imminent, and impending risk of injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his personal and financial information being placed in the hands of criminals.

10. Defendant Puma Biotechnolgy, Inc. ("Defendant" or "Puma") is a Delaware corporation headquartered at 10880 Wilshire Blvd., Los Angeles, CA 90024.

III. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2) and (3), because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of

the class is a citizen of a state different from Defendant, including Plaintiff Mfolozi Dlamini.

12. This Court has personal jurisdiction over the Defendant because Defendant has its principal place of business within this District.

13. Venue is proper in this District pursuant to 28 U.S.C. §1391(b)(2) because Defendant's headquarters is in this District, and it conducts much of its business throughout this District.

IV. FACTUAL ALLEGATIONS

Background

14. Defendant Puma is a large biopharmaceutical company that promotes itself as being a company that is "committed to protecting and respecting your privacy."[5]

15. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their sensitive PII and PHI.

16. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII and PHI from disclosure to third parties.

[5] *Id.*

The Data Breach

17. Between April 22, 2022 and June 19, 2022, unauthorized third-party cybercriminals infiltrated the systems that Puma uses to store sensitive personal information (including PII and PHI) of its customers (the "Data Breach").[6] These cybercriminals went undetected as they accessed PII and PHI including names, Social Security numbers, financial account information, and health insurance information.[7]

18. On or about mid-May 2023, roughly 11 full months later, Defendant transmitted to Plaintiff and Class Members the notice letter (the "Data Breach Notice") informing them of the Data Breach in which their PII and PHI was compromised.[8]

19. The Data Breach Notice stated that on "June 19, 2022, Puma discovered suspicious activity on [its] computer network."[9] In response, Defendant "launched an investigation with the assistance of third-party computer specialists to determine the nature and scope of the incident."[10] "On June 27, 2022, the investigation determined that certain files on Puma's systems were subject to

[6] Exhibit A.
[7] *Id.*
[8] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a193b9d8-f0ad-4f3b-952c-db1f3d322f39.shtml (last visited May 25, 2023). *See* also Exhibit A.
[9] *See* Exhibit A.
[10] *Id.*

unauthorized access and/or acquisition."[11] The investigation further determined that as a result of the Data Breach, unauthorized third-parties viewed, accessed, and exfiltrated Plaintiff's and Class Members' sensitive PII and PHI including their "Social Security number[s], financial account information, health insurance information, and name[s]."[12] This means that not only did the cybercriminals view and access the PII and PHI without authorization, but they also removed Plaintiff's and Class Members' PII and PHI. In the Data Breach, these criminals acquired the most damaging kind of PII and PHI that can be exposed to unauthorized third parties, including, but in no way limited to, Social Security numbers and sensitive medical information.

20. Due to Defendant's inadequate and insufficient data security measures, Plaintiff and Class Members now face an increased risk of fraud and identity theft and must live with that threat forever. Plaintiff believes his PII and PHI was both stolen in the Data Breach and is still in the hands of the cybercriminal "hackers." Plaintiff further believes his PII and PHI has already been sold on the Dark Web and downloaded following the Data Breach, as that is the *modus operandi* of cybercriminals who perpetrate cyberattacks of the type that occurred here.

21. Defendant had obligations to Plaintiff and Class Members to safeguard

[11] *Id.*
[12] *Id.*

their PII and PHI and to protect it from unauthorized access and disclosure.

22. Plaintiff and Class Members provided their PII and PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

23. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches of major companies preceding the date of the Data Breach.

24. Defendant knew or should have known that these attacks were common and foreseeable. In 2022, there were 1,802 data breaches, nearly eclipsing 2021's record wherein 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[13] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[14]

25. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential

[13] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6 (last visited May 25, 2023).

[14] See *Data Breaches Hit Lots More People in 2022* (Jan. 25, 2023) https://www.cnet.com/tech/services-and-software/data-breaches-hit-lots-more-people-in-2022/ (last visited May 25, 2023).

targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities . . . are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[15]

26. The increase in such attacks, and the resulting risk of future attacks, was widely known to the public and to anyone in the Defendant's industry, including Defendant.

Defendant Did Not Use Reasonable Security Procedures

27. Despite this knowledge, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, non-encrypted information it was maintaining for Plaintiff and Class Members, causing Plaintiff's and Class Members' PII and PHI to be exposed.

28. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

[15] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), *available at*: https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited May 25, 2023).

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/

LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

29. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce

malicious network traffic.[16]

30. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit
- Remove privileged credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise.

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely.

[16] *See* Cybersecurity & Infrastructure Security Agency, *Protecting Against Ransomware* (original release date Apr. 11, 2019), *available at:* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited May 25, 2023).

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords.

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[17]

[17] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited May 25, 2023).

31. Given that Defendant was storing the PII and PHI of Plaintiff and Class Members, Defendant could and should have implemented all the above measures to prevent and detect cyber-attacks.

32. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent "hacking" attacks, resulting in the Data Breach and the exposure of the PII and PHI of an undisclosed amount of current and former consumers, including Plaintiff and Class Members.

Securing PII and PHI and Preventing Breaches

33. Defendant could have prevented this Data Breach by properly securing and encrypting the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data that was no longer useful, especially outdated data.

34. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class Members was exacerbated by the repeated warnings and alerts directed to businesses to protect and secure sensitive data.

35. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

Defendant Failed to Comply with FTC Guidelines

36. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

37. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[18] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[19]

38. The FTC further recommends that companies not maintain PII and PHI

[18] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 25, 2023).
[19] *Id.*

longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

39. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

40. Defendant failed to properly implement basic data security practices.

41. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

42. Defendant was always fully aware of its obligation to protect the PII and PHI of Plaintiff and Class Members. Defendant was also aware of the significant repercussions that would result from their failure to do so.

Defendant Failed to Comply with Industry Standards

43. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices.

44. Other best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

45. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity

readiness.

46. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the Data Breach.

Value of Personally Identifiable Information

47. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[21]

48. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Personal Information can be

[20] 17 C.F.R. § 248.201 (2013).
[21] *Id*.

sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[22] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[23] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[24]

49. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until

---

[22] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited May 25, 2023).

[23] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited May 25, 2023).

[24] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited May 25, 2023).

> you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[25]

50. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

51. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[26]

52. Based on the foregoing, the information compromised in the Data

---

[25] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 25, 2022).

[26] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited May 25, 2023).

Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, Driver's License number, addresses, and financial information.

53. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[27]

54. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

55. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

[27] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited May 25, 2023).

56. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

57. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[28]

58. Moreover, the fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result,

[28] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed May 25, 2023)

studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

59. The PII and PHI stolen in the Data Breach have significant value, as PII and PHI is a valuable property right. [30] Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[31]

60. There is also an active and robust legitimate marketplace for PII. In 2019, the data brokering industry was worth roughly $200 billion.[32] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker, who in turn aggregates the information and provides it to marketers or app developers.[33] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[34]

---

[29] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited May 25, 2023).

[30] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets." (citations omitted)).

[31] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited May 25, 2023).

[32] David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak* (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited May 25, 2023).

[33] *See, e.g.*, https://datacoup.com/; https://worlddataexchange.com/about.

[34] Computer & Mobile Panel, NIELSEN, *available at* https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing (last visited May 25, 2023).

61. As a result of the Data Breach, Plaintiff's and Class Members' PII and PHI, which has an inherent market value in both legitimate and black markets, has been damaged and diminished by its unauthorized release to third party actors, to whom it holds significant value. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII and PHI are now readily available, and the rarity of Plaintiff's and Class Members' PII and PHI has been lost, thereby causing additional loss of value.

62. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members, names, Social Security numbers, financial account information, and health insurance information, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

63. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

64. Defendant was, or should have been, fully aware of the unique type

and the significant volume of data on Defendant's server(s) and computer network, amounting to potentially millions of individuals' detailed PII and PHI, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

65. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiff and Class Members. The ramifications of Defendant's failure to keep secure the PII and PHI of Plaintiff and Class Members are long lasting and severe. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years.

V. PLAINTIFF-SPECIFIC ALLEGATIONS

Plaintiff Mfolozi Dlamini Experience

66. Plaintiff Mfolozi Dlamini was an employee of Defendant from August 2020 until July 2021. As a condition of his employment with Defendant, Plaintiff Dlamini was required to provide his personally identifying information ("PII") and Private Health Information ("PHI") to Defendant which was then entered into Defendant's database and maintained by Defendant.

67. Plaintiff greatly values his privacy and PII and PHI, especially when providing this sensitive information to his employer. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of his PII and PHI.

68. Plaintiff received a letter dated May 17, 2023 from Defendant concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Defendant's systems that contained his name, Social Security number, financial account information, and health insurance information.

69. Since learning of the Data Breach, Plaintiff has spent additional time reviewing his bank statements, medical information and statements, and credit cards. Since the date of the breach, he has spent approximately three hours reviewing his accounts and credit reports. Defendant has also spent valuable time signing up for the credit monitoring service offered by Epiq.

70. Plaintiff has experienced an increase of other spam calls, text messages and emails after the Data Breach.

71. Plaintiff has noticed a sharp increase in suspicious advertisements on his social media accounts and has been forced to change all social media account passwords.

72. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has not been forthright with information about the Data Breach.

73. Plaintiff plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

74. Additionally, Plaintiff is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

75. Plaintiff stores any documents containing his PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

76. Plaintiff has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff's Injuries and Damages

77. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members are presently experiencing and will continue experiencing actual harm from fraud and identity theft.

78. Plaintiff and Class Members are presently experiencing substantial risk of out-of-pocket fraud losses, such as loans opened in their names, tax return fraud, utility and medical bills opened in their names, and similar identity theft.

79. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII and PHI as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

80. Plaintiff and Class Members are also incurring and may continue incurring out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

81. Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by the cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

82. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant and their affiliates was intended to be used by Defendant to fund adequate security of Defendant's computer property and protect Plaintiff's and Class Members' PII and PHI. Thus, Plaintiff and Class Members did not get what they paid for.

83. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

84. Plaintiff and Class Members have suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy

or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring medical insurance accounts, bank accounts, payment card statements, and credit reports for unauthorized activity for years to come.

85. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII and PHI, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential personal, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

86. Further, as a result of Defendant's conduct, Plaintiff and Class

Members are forced to live with the anxiety that their PII and PHI may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

87. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a substantial and present risk of harm.

VI. CLASS ALLEGATIONS

88. Pursuant to FRCP 23(b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of the following nationwide class ("Nationwide Class"):

> **All persons in the United States whose personal information was compromised in the data breach publicly announced by Puma in April 2023.**

89. Excluded from the proposed Class are Defendant, including any entity in which Defendant has a controlling interest, is a subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded from the proposed Class are the judge to whom this case is assigned and any members of his or her judicial staff and immediate family.

90. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division, or create and seek certification of additional

classes, after having had an opportunity to conduct discovery.

91. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class wide relief because Plaintiff and all members of the Class were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

92. **Numerosity.** The Class Members are so numerous that the joinder of all members is impracticable. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

93. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of

Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual damages, nominal damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

94. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII and PHI, like that of every other Class member, was compromised in the Data Breach.

95. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

96. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

97. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal

litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, treating this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

98. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

99. Likewise, particular issues under Federal Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII and PHI;

b. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data

security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII and PHI; and

e. Whether adherence to FTC data security recommendations and measures recommended by data security experts would have reasonably prevented the data breach.

100. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

101. Plaintiff incorporates by reference all previous allegations in paragraphs 1-100 as though fully set forth herein.

102. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

103. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

104. Defendant had full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if the data were wrongfully disclosed.

105. By assuming responsibility for collecting and storing this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII and PHI held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious time period and to give prompt notice to those affected in the case of a data breach.

106. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

107. Defendant was subject to an "independent duty," untethered to any

contract between Defendant and Plaintiff or Class Members.

108. A breach of security, unauthorized access, and resulting injury to Plaintiff's and Class Members' PII and PHI was reasonably foreseeable, particularly considering Defendant's inadequate security practices, which includes sharing and/or storing the PII and PHI of Plaintiff and Class Members on its computer systems.

109. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and Class Members, the critical importance of providing adequate security of that data, and the necessity for encrypting all data stored on Defendant's systems.

110. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and Class Members, including basic encryption techniques freely available to Defendant.

111. Plaintiff and Class Members had no ability to protect their PII and PHI that was in, and probably remains in, Defendant's possession.

112. Defendant was able to protect against the harm suffered by Plaintiff

and Class Members as a result of the Data Breach.

113. Defendant had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

114. Defendant had a duty to comply with the industry standards set out above.

115. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII and PHI within Defendant's possession.

116. Defendant, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII and PHI.

117. Defendant, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class Members that the PII

and PHI within Defendant's possession might have been compromised and precisely the type of information compromised.

118. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII and PHI to be compromised.

119. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding the type of PII and PHI that has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

120. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, fraud, loss of time and money to monitor their finances for fraud, and loss of control over their PII and PHI.

121. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of present and continuing harm in that their PII and PHI, which is still in the possession of third parties, will be used for fraudulent purposes. Plaintiff and Class Members will need identity theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the PII and PHI at issue, which includes sensitive medical information.

122. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiff and Class

Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII and PHI of Plaintiff and Class Members was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI, by adopting, implementing, and maintaining appropriate security measures.

123. Plaintiff seeks the award of actual damages on behalf of themselves and the Class.

124. In failing to secure Plaintiff's and Class Members' PII and PHI and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

125. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling Defendant to institute appropriate data collection and safeguarding methods and policies regarding customer information.

COUNT II
Negligence *per se*
(On Behalf of Plaintiff and the Class)

126. Plaintiff incorporates by reference all previous allegations in paragraphs 1-100 as though fully set forth herein.

127. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies like Defendant of failing to use reasonable measures to protect PII and PHI.

128. The FTC publications and orders also form the basis of Defendant's duty to the Class.

129. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and PHI and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI that it obtained and stored and the foreseeable consequences of a data breach of that data.

130. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

131. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

132. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

133. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

134. Plaintiff incorporates by reference all previous allegations in paragraphs 1-100 as though fully set forth herein.

135. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

136. Defendant owed a duty to Plaintiff and Class Members to keep their PII and PHI confidential.

137. Defendant intentionally failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII and PHI of Plaintiff and Class Members.

138. Defendant allowed unauthorized and unknown third parties access to and examination of the PII and PHI of Plaintiff and Class Members, by way of Defendant's failure to protect the PII and PHI.

139. The unauthorized release to, custody of, and examination by

unauthorized third parties of the PII and PHI of Plaintiff and Class Members is highly offensive to a reasonable person.

140. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII and PHI to Defendant as part of their relationships with Defendant, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

141. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or

as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

142. Defendant acted with intention and a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that their information security practices were inadequate and insufficient.

143. Because Defendant acted with this knowing state of mind, it had noticed and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

144. As a proximate result of the above acts and omissions of Defendant, PII and PHI of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

145. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

146. Plaintiff incorporates by reference all previous allegations in paragraphs 1-100 as though fully set forth herein.

147. Plaintiff and Class Members conferred a monetary benefit to Defendant by paying Defendant for its services.

148. Defendant knew that Plaintiff and Class Members conferred a monetary benefit to Defendant when it accepted and retained that benefit.

149. Defendant was supposed to use some of the monetary benefit provided to it from Plaintiff and Class Members to secure the PII and PHI belonging to

Plaintiff and Class Members by paying for costs of adequate data management and security.

150. Defendant should not be permitted to retain any monetary benefit as a result of its failure to implement necessary security measures to protect the PII and PHI of Plaintiff and Class Members.

151. Defendant gained access to Plaintiff's and Class Members' PII and PHI through inequitable means because Defendant failed to disclose that it used inadequate security measures.

152. Plaintiff and Class Members were unaware of the inadequate security measures and would not have provided their PII and PHI to Defendant had they known of the inadequate security measures.

153. To the extent that this cause of action is pled in the alternative to the others, Plaintiff and Class Members have no adequate remedy at law.

154. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate

the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

155. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

156. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds from the monetary benefit that it unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the PII and PHI of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train their security personnel

regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess their

respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of

the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, treble, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

DATED: May 26, 2023

Respectfully submitted,

By, */s/ M. Anderson Berry*

M. Anderson Berry (262879)
Gregory Haroutunian (330263)
Brandon P. Jack (325584)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
6200 Canoga Ave, Suite 375
Woodland Hills, CA 91367
Telephone: (747) 777-7748
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Justin Walker (*Pro Hac Vice* Forthcoming)

MARKOVITS, STOCK & DEMARCO, LLC
119 E. COURT STREET, SUITE 530
CINCINNATI, OHIO 45202
119 E. Court Street, Suite 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
jwalker@msdlegal.com

Exhibit A

Return Mail Processing Center
P.O. Box 3826
Suwanee, GA 30024

5 1 742 **********AUTO**MIXED AADC 300
Mfolozi Dlamini
REDACTED
REDACTED

May 17, 2023

NOTICE OF SECURITY INCIDENT

Dear Mfolozi Dlamini:

Puma Biotechnology, Inc. ("Puma") writes to notify you of a recent incident that may affect the privacy of some of your information. We are providing you with information about the incident, our ongoing response, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On June 19, 2022, Puma discovered suspicious activity on our computer network. We immediately secured our network and launched an investigation with the assistance of third-party computer specialists to determine the nature and scope of the incident. On June 27, 2022, the investigation determined that certain files on Puma's systems were subject to unauthorized access and/or acquisition. As a result, and in an abundance of caution, we undertook a diligent and comprehensive review to determine the information present on the network that may have been contained within impacted files and potentially subject to unauthorized access and/or acquisition. On March 16, 2023, we received results from this review. We then conducted a comprehensive internal evaluation of the information in order to confirm data elements, populate address information for impacted individuals, and confirm accuracy. This process was completed on May 5, 2023 and we have confirmed the files contained certain information related to you.

What Information Was Involved? The investigation determined that your Social Security number, financial account information, health insurance information, and name may have been subject to unauthorized access and/or acquisition. To the best of our knowledge, there is no indication that your information was actually or attempted to be misused as a result of this incident.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. Upon learning of this incident, we moved quickly to investigate and respond, assess the security of our systems, and notify potentially affected individuals. As part of our ongoing commitment to the security of information, we are reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future incident. We reported this incident to federal law enforcement and will comply with any investigation. We will also be notifying state and federal regulators, as required.

As an added precaution, we are also offering you complimentary access to 12 months of credit monitoring and identity theft restoration services through Epiq. We encourage you to strongly consider activating these services as we are not able to act on your behalf to activate them for you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. We encourage you to remain vigilant against identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You can find out more about how to protect your information in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will also find more information on the credit monitoring services we are offering and how to enroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions or need assistance, please call us at 866-870-0474 Monday through Friday between the hours of 9 am to 9 pm ET excluding U.S. holidays.

We take this incident very seriously and sincerely regret any inconvenience or concern this incident caused you.

Sincerely,

Puma Biotechnology, Inc.